23P306S (Pages: 2) Name: .....

Reg.No: .....

THIRD SEMESTER M.Sc. DEGREE EXAMINATION, NOVEMBER 2024

(CBCSS - PG)

CC19P CSS3 E02C - CRYPTOGRAPHY AND NETWORK SECURITY

(Computer Science)

(2019 Admission - Supplementary/Improvement)

Time : 3 Hours Maximum : 30 Weightage

Part-A

Answer any ***four*** questions. Each question carries 2 weightage.

1. Illustrate stream cipher structure with figure.
2. Explain secure hash function and its requirements.
3. Describe Public-Key Certificates.
4. Describe Federated Identity Management.
5. Explain ESP Packet format with neat figure.
6. Explain Distributed Intrusion Detection technique.
7. Explain firewall characteristics.

(4 × 2 = 8 Weightage)

Part-B

Answer any ***four*** questions. Each question carries 3 weightage.

8. Explain security attacks with neat figures.
9. Discuss AES briefly.
10. Describe CCM mode of operation.
11. Explain Diffie-Hellman Key Exchange.
12. Discuss SSL Record Protocol and Change Cipher Spec Protocol.
13. Explain applications, services and benefits of IPsec.
14. Describe VPN.

(4 × 3 = 12 Weightage)

Part-C

Answer any ***two*** questions. Each question carries 5 weightage.

15. Summarize Fiestel Cipher Structure.
16. Illustrate Kerberos version 4 in detail.
17. Explain how TLS makes use of pseudorandom function.

18. Illustrate Worms and Viruses in detail.

(2 × 5 = 10 Weightage)

****